UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/577,005	07/05/2006	Hagen Ploog	3000-0052	7521

50811 7590 12/21/2007

O'SHEA, GETZ & KOSAKOWSKI, P.C.
1500 MAIN ST.
SUITE 912
SPRINGFIELD, MA 01115

EXAMINER	
LAFORGIA, CHRISTIAN A	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
12/21/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/577,005	**Applicant(s)** PLOOG ET AL.	
	Examiner Christian La Forgia	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 April 2006*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5 and 7-20* is/are rejected.

7)☒ Claim(s) *6* is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *24 April 2006* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *4/24/06;7/5/06;11/5/07*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. Claims 1-20 have been presented for examination.

Priority

2. Acknowledgment is made of applicant's claim for foreign priority. ***Information***

Disclosure Statement

3. The information disclosure statements (IDS) submitted on 24 April 2006, 05 July 2006, and 05 November 2007 are in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statements have been considered by the examiner.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1, 2, 7, 10, and 15 are rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent Application Publication No. 2003/0084308 A1 to Van Rijnswou, hereinafter Van Rijnswou.

6. As per claim 1, Van Rijnswou teaches a method of storing encrypted data in a random access memory, comprising the steps of:

encrypting data word by permutating each data bit of the data word using a permutation key (i.e. hashed address) to generate permutated data word (paragraph 0018, i.e. hashing the address, combining the hashed address with the word D using an exclusive-OR, and encrypting using DES), and storing the permutated data word in the memory (Figure 2 [block 30], paragraph 0018).

7. Regarding claim 2, Van Rijnswou teaches after the step of permutating, substituting each data bit of the permutated data word using a substitution key to generate a substitute data word (paragraph 0018, i.e. DES involves a substitution step as noted by p. 274 of **Applied Cryptography**, by Bruce Schneier, hereinafter Schneier), and

where the step of storing comprises the step of storing the substitute data word in the memory (Figure 2 [block 30], paragraph 0018).

8. Regarding claim 3, Van Rijnswou teaches substituting each data bit of the unencrypted data word using a substitution key prior to the step of permutating to generate a substitute data word (paragraph 0018), and

where the step of permutating comprises the step of permutating each data bit of the substitute data word using the permutation key to generate the permutated data word (paragraph 0018, i.e. bit-wise XOR).

9. With regards to claim 7, Van Rijnswou teaches where the substitution key includes a plurality of key bits corresponding to the number of data bits of the permutated data word, where the step of substituting each data bit of the permutated data word using a substitution key (paragraph 0018, i.e. hashed address having a plurality of bits) further comprises

the step of mapping each data bit of the permutated data word to a data bit of the substituted data word in one of an unchanged form and an inverted form as determined by the corresponding one of these key bits (paragraph 0018, i.e. performing a bit-wise XOR between the hashed address information and the data).

10. Regarding claim 10, Van Rijnswou teaches decrypting the stored permutated data word using a second permutation key matched to the permutation key used to generate the permutated data word (paragraphs 0019-0020).

11. As per claim 15, Van Rijnswou teaches a method of storing encrypted data in a memory, comprising the steps of:

encrypting a data word by permutating each data bit of the data word using a permutation key to generate a permutated data word (paragraph 0018, i.e. hashing the address, combining the hashed address with the word D using an exclusive-OR, and encrypting using DES);

substituting each data bit of the permutated data word using a substitution key to generate a substitute data word (paragraph 0018, i.e. DES involves a substitution step as noted by p. 274 of Schneier); and

storing the substitute data word in the memory (Figure 2 [block 30], paragraph 0018).

Claim Rejections - 35 USC § 103

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

13. Claims 4, 5, 8, 9, 11-14, 16, 17, 19, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Van Rijnswou in view of U.S. Patent No. 5,995,623 to Kawano et al., hereinafter Kawano.

14. Regarding claims 4, 16, and 19, Van Rijnswou teaches assigning each one of the subkeys to a corresponding one of the data bits of the permutated data word (paragraph 0018, i.e. bit-wise XOR); and

mapping each data bit of the unencrypted data word to a corresponding one of the data bits of the permutated data word using the corresponding assigned subkey (paragraph 0018, i.e. bit-wise XOR).

15. Van Rijnswou does not teach where the permutation key includes a plurality of subkeys corresponding to the number of the data bits of the data word, and where each one of the subkeys includes a plurality of key bits where the step of permutating each data bit in the data word using a permutation key.

16. Kawano teaches selecting an encryption key (Figure 3 [step 3]), encrypting the data bit by bit (Figure 3 [steps 4 and 5]), and selecting a different key for a different set of bits (Figure 3 [step 3]) (Figures 4A-4E, 8, column 11, lines 1-34).

17. It would have been obvious to one of ordinary skill in the art at the time the invention was made to have the permutation key include a plurality of subkeys corresponding to the number of the data bits of the data word, and where each one of the subkeys includes a plurality of key bits where the step of permutating each data bit in the data word using a permutation key, since Kawano states at column 5, lines 22-25 that such a method provides a high level of security with small computation costs and simple key administration.

18. With regards to claims 5, 17, and 20, Kawano teaches where the step of mapping comprises:

a) selecting a first group of the data bits of the data word determined by a first one of the plurality of key bits of the corresponding assigned subkey (Figures 3 [steps 2-5], column 10, lines 43-67, column 11, lines 1-34);

b) selecting a second group of the data bits of the data word from the first group of the data bits as determined by a second one of the plurality of key bits of the corresponding assigned subkey (Figure 3 [steps 2-5], column 10, lines 43-67, column 11, lines 1-34, i.e. the steps would be the same for any subsequent group); and

c) repeating step b), each time using an additional one of the plurality of key bits of the corresponding assigned subkey until there exists one remaining data bit of the data word, where the one remaining data bit corresponds to the data bit of the data word mapped to the corresponding data bit of the permutated data word (column 11, lines 35-50).

19. With regards to claim 8, Van Rijnswou does not teach where the substitution key includes a plurality of key bits corresponding to the number of data bits of the data word, where the step of substituting each data bit of the data word using a substitution key further comprises the step of mapping each data bit of the data word to a data bit of the substituted data word in one of an unchanged form and an inverted form as determined by the corresponding one of the key bits.

20. Kawano teaches where the substitution key includes a plurality of key bits corresponding to the number of data bits of the data word (Figures 3 [steps 2 and 3], 4C [block 33], column 10, lines 43-67, column 11, lines 1-34),

where the step of substituting each data bit of the data word using a substitution key (figure 3 [steps 3, 4], column 10, lines 43-67, column 11, lines 1-34) further comprises

the step of mapping each data bit of the data word to a data bit of the substituted data word in one of an unchanged form and an inverted form as determined by the corresponding one of the key bits (Figure 3 [step 5], column 10, lines 43-67, column 11, lines 1-34).

21. It would have been obvious to one of ordinary skill in the art at the time the invention was made to have the substitution key include a plurality of key bits corresponding to the number of data bits of the data word, where the step of substituting each data bit of the data word using a substitution key further comprises the step of mapping each data bit of the data word to a data bit of the substituted data word in one of an unchanged form and an inverted form as determined by the corresponding one of the key bits, and where each one of the subkeys includes a plurality of key bits where the step of permutating each data bit in the data word using a permutation key, since Kawano states at column 5, lines 22-25 that such a method provides a high level of security with small computation costs and simple key administration.

22. Regarding claim 9, Van Rijnswou does not teach generating the permutation key by the following steps: a) randomly generating a sub-permutation-key and assigning the generated sub-permutation-key to a data bit position of the permutated data word; b) checking whether the generated sub-permutation-key has already been assigned to a data bit of the permutated data word, and retaining the generated sub-permutation-key as the assigned sub-permutation-key if the generated sub-permutation key has not yet been assigned to a data bit of the permutated data word; and c) implementing steps a) and b) until a sub-permutation-key is assigned to each data bit of the permutated data word.

23. Kawano teaches generating the permutation key by the following steps:

a) randomly generating a sub-permutation-key and assigning the generated sub-permutation-key to a data bit position of the permutated data word (Figures 3 [steps 2 and 3], 4C [block 33], column 10, lines 43-67, column 11, lines 1-34);

b) checking whether the generated sub-permutation-key has already been assigned to a data bit of the permutated data word, and retaining the generated sub-permutation-key as the assigned sub-permutation-key if the generated sub-permutation key has not yet been assigned to a data bit of the permutated data word (figure 3 [steps 3, 4], column 10, lines 43-67, column 11, lines 1-34); and

c) implementing steps a) and b) until a sub-permutation-key is assigned to each data bit of the permutated data word (column 11, lines 35-50).

24. It would have been obvious to one of ordinary skill in the art at the time the invention was made to generate the permutation key in the manner claimed above, since Kawano states at column 5, lines 22-25 that such a method provides a high level of security with small computation costs and simple key administration.

25. As per claim 11, Van Rijnswou teaches a device that encrypts and decrypts a data word having a predetermined number of data bits (Abstract), the device having a permutation unit comprising:

a plurality of data inputs that receive the data bits of the data word (Figure 2 [element 26], paragraph 0018).

26. Van Rijnswou does not teach a plurality of selection units corresponding to the number of data bits of the data word, where each one of the selection units is responsive to a subkey portion of a permutation key, where each one of the selection units provides one data bit each of a permutated data word from the corresponding data bit of the data word as determined by the corresponding one of the subkeys.

27. Kawano teaches selecting bits from a data word and encrypting the various bits using different keys (Figures 3, 4A-4E, column 10, lines 43-67, column 11, lines 1-34).

28. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include a plurality of selection units corresponding to the number of data bits of the data word, where each one of the selection units is responsive to a subkey portion of a permutation key, where each one of the selection units provides one data bit each of a permutated data word from the corresponding data bit of the data word as determined by the corresponding one of the subkeys, since Kawano states at column 5, lines 22-25 that such a method provides a high level of security with small computation costs and simple key administration.

29. Regarding claim 12, Kawano teaches where each selection units comprises number of consecutively arranged selection stages corresponding to a number of permutation key bits of the corresponding subkey for that selection unit, where a first selection stage is responsive to a first one of the permutation key bits to select and provide a first group of data bits of the data word, and where subsequent ones of the selection stages are each responsive to subsequent ones of the permutation key bits to select a subgroup of the data bits from a group of data bits of the data word provided by the respective previous selection stage (column 10, lines 43-67, column 11, lines 1-34).

30. Regarding claims 13 and 14, Van Rijnswou teaches a substitution unit connected after or after the permutation unit, that substitutes each data bits of the permutated data word in response to a substitution keys (paragraph 0018, i.e. DES involves a substitution step as noted by p. 274 of Schneier).

31. It would have been obvious to one of ordinary skill in the art at the time the invention was made to perform the substitution before or after the permutation, since it has been held that the selection of any order of performing steps is a *prima facie* case of obviousness in the absence of new or unexpected results. See MPEP § 2144.04(IV); see also *In re Burhans*, 154 F.2d 690, 69 USPQ 330 (CCPA 1946).

32. Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over Van Rijnswou.

33. As per claim 18, Van Rijnswou teaches a method of storing encrypted data in a memory, comprising the steps of:

substituting each data bit of an unencrypted data word using a substitution key to generate a substitute data word (paragraph 0018, i.e. DES involves a substitution step as noted by p. 274 of Schneier); and

permutating each data bit of the substitute data word using a permutation key to generate a permutated data word (paragraph 0018, i.e. hashing the address, combining the hashed address with the word D using an exclusive-OR, and encrypting using DES);

storing the permutated data word in the memory (Figure 2 [block 30], paragraph 0018).

34. Van Rijnswou does not teach method steps in the order claimed by applicant.

35. It would have been obvious to one of ordinary skill in the art at the time the invention was made to rearrange the process steps of Van Rijnswou to the order claimed by the Applicant, since it has been held that the selection of any order of performing steps is a *prima facie* case of obviousness in the absence of new or unexpected results. See MPEP § 2144.04(IV); see also *In re Burhans*, 154 F.2d 690, 69 USPQ 330 (CCPA 1946).

Allowable Subject Matter

36. Claim 6 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

37. The following is a statement of reasons for the indication of allowable subject matter: The Examiner cannot find prior art that would show data being reduced by a factor of two each time it is encrypted with a new key. At the same time, the Examiner does not know of anything and cannot find anything that would render obvious the abovementioned limitation.

Conclusion

38. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

39. The following patents are cited to further show the state of the art with respect to encrypting data to be stored in memory, such as:

United States Patent No. 6,701,418 B2 to Poletto et al., which is cited to show address correction for shared memory systems.

United States Patent No. 5,860,094 to Junya, which is cited to show protecting data stored on physical media.

United States Patent No. 5,249,232 to Erbes et al., which is cited to show an encryption device for encrypting data to be written to main memory.

United States Patent Application Publication No. 2005/0044392 A1 to Gammel et al., which is cited to show key management for the encryption of data words stored in memory.

United States Patent Application Publication No. 2006/0265563 A1 to Goettfert et al., which is cited to show generating a key for each word to be encrypted and stored in memory.

United States Patent No. 5,915,025 to Taguchi et al., which is cited to show encrypting data to be stored in memory.

40. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

41. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

42. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christian LaForgia
Patent Examiner
Art Unit 2131

Clf